REMARKS

Claims 1-5 have been amended. Claims 1-16 remain pending in the application. Reconsideration is respectfully requested in light of the following remarks.

Section 112, First Paragraph, Rejection:

The Examiner rejected claims 1, 6, 11 and 16 under 35 U.S.C. § 112, first paragraph, as failing to comply with the written description requirement. Applicants respectfully traverse this rejection for at least the following reasons.

The Examiner incorrectly asserts that "the word 'quiesce' is very rarely used." The term "quiesce" is frequently used with a well understood meaning in the art of storage technology that is consistent with how the term is used in Applicants' claims. Applicants' usage of the word "quiesce" is consistent with conventions readily understood and accepted by those skilled in the relevant arts of storage technology.

Applicants draw the Examiner's attention to para. 0006 of the specification which states:

> In distributed shared storage environments where multiple clients may need simultaneous access to the same data, datasets may be fixed into specific versions to ensure data integrity across client sessions. These dataset versions may be referred to as file images. Certain tasks, like backing up one or more files, checking and correcting data consistency across mirrored database files, or virus removal may require a single application or process to have exclusive access to one or more file images. Typically, general access to the datasets involved must be quiesced and all data caches must be flushed. (emphasis added).

Thus, the phraseology use in Applicants' independent claims is clearly supported in the specification. Applicants respectfully remind the Examiner that it is well settled law that the claimed invention does not have to be described in *ipsis verbis* in order to satisfy the description requirement of §112. *Jacobs v. Lawson*, 214 USPQ 907, 910 (B.P.A.I. 1982). "The subject matter of the claim need not be described literally in order for the disclosure

to satisfy the description requirement." *M.P.E.P. 2163.02*. As longs as the description "allows persons of ordinary skill in the art to recognize that [the inventors] invented what is claimed" then the description requirement is satisfied. *In re Gosteli*, 10 USPQ2d 1614, 1618 (Fed. Cir. 1989). Moreover, the section 112 description requirement may be satisfied by principles of inherency. *In re Reynolds*, 443 F.2d 384 (CCPA 1971). As shown above, Applicants' claims are clearly in complete compliance with the requirements of 35 U.S.C. § 112, first paragraph. Withdrawal of this rejection is respectfully requested.

Section 101 Rejection:

The Examiner rejected claims 1-5 (Applicants' assume inclusion of claims 6-22 in the rejection was a typographical error since these claims were not discussed and claims 17-22 do not exist) under 35 U.S.C. § 101 as not being directed to statutory subject matter. Applicants' respectfully traverse this rejection. However, in order to expedite prosecution, claim 1 has been amended to recite a "computer-implemented" method. Withdrawal of this rejection is respectfully requested.

Section 103(a) Rejection:

The Examiner rejected claims 1, 3-6, 8-11 and 13-15 under 35 U.S.C. § 103(a) as being unpatentable over Schmeidler et al. (U.S. Patent 6,374,402) (hereinafter "Schmeidler") in view of Hart (U.S. Patent 6,983,295), and claims 2, 7, 12 and 16 as being unpatentable over Schmeidler in view of Hart and further in view of McBrearty et al. (U.S. Publication 2004/0015585) (hereinafter "McBrearty"). Applicants respectfully traverse these rejections for at least the following reasons.

In rejecting the claims under 35 U.S.C. 103(a), the Examiner improperly engages in a piecemeal examination of fragments of the Applicants' claims, matching the fragments to isolated bits of prior art references, with both elements removed from their original context. Applicants respectfully remind the Examiner that both the claims and

the each prior art reference must be considered as a whole. "In determining the differences between the prior art and the claims, the question under 35 U.S.C. 103 is not whether the differences **themselves** would have been obvious, but whether the claimed invention as a whole would have been obvious." *Stratoflex, Inc. v. Aeroquip Corp.*, 713 F.2d 1530, 218 USPQ 871 (Fed. Cir. 1983); *Schenck v. Nortron Corp.*, 713 F.2d 782, 218 USPQ 698 (Fed. Cir. 1983). Also, a prior art reference must be considered in its entirety, i.e., as a whole, including portions that would lead away from the claimed invention. *W.L. Gore & Associates, Inc. v. Garlock, Inc.*, 721 F.2d 1540, 220 USPQ 303 (Fed. Cir. 1983), *cert. denied*, 469 U.S. 851 (1984). As further shown below, the Examiner is clearly attempting a piecemeal reconstruction of Applicants' invention without consider the claimed invention as a whole. Such reconstruction is improper. *See, e.g., Interconnect Planning Corp. v. Feil*, 774 F.2d 1132, 1143, 227 USPQ 543, 551 (Fed. Cir. 1985) (it is insufficient to select from the prior art the separate components of the inventor's combination, using the blueprint supplied by the inventor). The Examiner cannot use the claimed invention as an instruction manual or "template" to piece together the teachings of the prior art so that the claimed invention is rendered obvious. *In re Fritch*, 23 USPQ 2d 1780, 1784 (Fed. Cir. 1992). "One cannot use hindsight reconstruction to pick and choose among isolated disclosures in the prior art to deprecate the claimed invention." *In re Fine*, 837 F.2d 1071, 1075, 5 USPQ 2d 1596, 1600 (Fed. Cir. 1988).

Regarding claim 1, the cited art fails to disclose, *in response to a metadata server receiving a data access request from a client, the metadata server determining a maximum expiration time indicated by a next scheduled quiesce time, wherein the data access request is for data that is also accessible by one or more other clients each having a corresponding unexpired token, and wherein said quiesce time is a time when exclusive access to the data is required by a task; generating an access token that grants the client access to data stored on one or more storage devices associated with the metadata server, wherein the access token comprises an expiration time; and wherein said generating an access token comprises setting the expiration time of the access token to be no later than the maximum expiration time indicated by a next scheduled quiesce time.*

Schmeidler's teachings are in regard to a Secure Content Delivery Platform (SCDP) for transactions between a user and a virtual storefront. As these secure transactions progress, a user's title is formatted into an electronic package that contains the title's files in a compressed and encrypted form, referred to as a briq. The briq is actually a portable, self-contained file system, containing all of the files necessary to run a particular title. Briqs are stored on a network file server, called a RAFT server. The SCDP client software uses a proprietary Random Access File Transport (RAFT) protocol and associated RAFT authorization token which the user obtains from a Conditional Access Server (CAS). The RAFT authorization token is a signed message from the CAS indicating that the requesting user can have access to a specified briq, on a specific RAFT file server, for the length of time spelled out in the negotiated payment type. The secure content edifice of Schmeidler incorporates an essential encryption mechanism, with an associated RAFT protocol and RAFT authorization tokens.

In the portions cited by the Examiner, Schmeidler is describing the proprietary RAFT (Random Access File Transport) encryption protocol used with RAFT authorization tokens, along with the data structure of the RAFT authorization tokens, and their digital signing and passing. Such encryption protocols, and their associated tokens, are common in secure transactions over computer networks. They have no particular bearing on Applicants' claims 1, 6, and 11.

The Examiner cites Schmeidler as teaching "determining a maximum expiration time indicated by a next scheduled quiesce time." Here, too, the reference is lifted from the context of Schmeidler and incorrectly applied to a fragmentary phrase found in claims 1, 6, and 11 of Applicants' invention. The cited text of Schmeidler on RAFT Tokens refers to an encryption protocol and associated data structure for a token authorizing access to a network file server. It does not teach or suggest **determining a maximum expiration time indicated by a next scheduled quiesce time**. **The disclosure of Schmeidler has nothing whatsoever to do with times of quiescence, or calculating an expiration time for an access token indicated by a time of quiescence.** Schmeidler

addresses secure transactions between a client computer and a content server, not the quiescing of data I/O in a distributed shared storage environment.

Citing the same portions of Schmeidler, the Examiner asserts that Schmeidler teaches "wherein said generating an access token comprises setting the expiration time of the access token to be no later than the maximum expiration time." Again, the above arguments refuting this assertion apply. Furthermore, the maximum expiration time of the Applicants' claims is indicated by a next scheduled quiesce time, wherein the quiesce time is a time when exclusive access is required by a task to the data that is accessible to multiple clients. The Examiner cites Hart at column 16, lines 53-54, to assert that Hart teaches "quiesce time is a time when exclusive access to the data is required by a task." However, the combination of Schmeidler and Hart clearly fail to teach or suggest a metadata server generating an access token that grants the client access to data stored on one or more storage devices associated with the metadata server, wherein generating the access token comprises setting the expiration time of the access token to be no later than the maximum expiration time indicated by a next scheduled quiesce time, wherein the quiesce time is a time when exclusive access is required by a task to the data that is accessible to multiple clients. Hart is refering to a "QUIESCE Time Stamp," which is simply a time stamp stored in a "file to indicate when a data disk means (D1) was taken off-line," as Hart discusses in his claim 1. **Neither Hart nor Schmeidler suggests the use of a next scheduled quiesce time to indicate a maximum expiration time for an access token generated by a metadata server in response to a data access request from a client for data that is also accessible by one or more other clients.**

Finally, Examiner asserts that "it would have been obvious to one of ordinary skill in the data processing art at the time of the invention, to have combine (sic) the teachings of the cited references because Hart's teachings would have allowed Schmeidler's method to provide a recovery method that can be measured in minutes (col. 2, lines 53-54)." However, the ability of Hart's system to perform recovery in minutes does not suggest the use of a next scheduled quiesce time to indicate a maximum expiration time for an access token generated by a metadata server in response to a data access request from a client for data

that is also accessible by one or more other clients. The reasoning provided by the Examiner is not relevant to the particular modification the Examiner is attempting to make to the prior art. Moreover, the systems of Schmeidler and Hart are completely different types of systems.

For at least the reasons above, the rejection of claim 1 is not supported by the cited art and removal thereof is respectfully requested. Similar remarks also apply to claims 6 and 11.

Regarding claim 16, Schmeidler in view of Hart and McBrearty fails to teach or suggest setting the expiration time of an access token to the earlier of either a maximum expiration time indicated by a next scheduled quiesce time or the default expiration time, wherein the access token grants a client access to data stored on one or more storage devices associated with a metadata server; and receiving a data I/O request associated with the access token, wherein the data I/O request is for data that is also accessible by one or more other clients each having a corresponding unexpired token, and wherein said quiesce time is a time when exclusive access to the data is required by a task. As discussed above in regard to claim 1, the cited art does not suggest the use of a next scheduled quiesce time to indicate a maximum expiration time for an access token generated by a metadata server in response to a data access request from a client for data that is also accessible by one or more other clients.

Further regarding claim 16, Schmeidler in view of Hart and McBrearty fails to teach or suggest determining a default expiration time and if the default expiration time is earlier than the maximum expiration time, setting the expiration time of the access token to be the default expiration time. The Examiner relies on McBrearty, citing paragraph [0004], to teach determining a default expiration time and if the default expiration time is earlier than the maximum expiration time, setting the expiration time of the access token to be the default expiration time. However, the Examiner's reliance on McBrearty is misplaced. McBrearty, even if combined with Schmeidler and Hart, does not teach or suggest determining a default expiration time and further fails to teach or suggest setting

the expiration time of the access token to the default expiration time if the default expiration time is earlier than the maximum expiration time.

McBrearty teaches a system to control access to a token server system that includes tokens with time specific permissions. McBrearty describes that each token may be encoded with "a tiny database" that, "lists exceptions and exclusions of function (e.g., read, write, execute) tied to specific time periods" (parentheses added, McBrearty, paragraph [0021]). In other words, McBrearty encodes a lookup table listing various time periods during which individual functions, such as reading, writing or executing, may not be performed. McBrearty does not describe how the specific time periods or the overall expiration time is determined.

The Examiner cites paragraph [0004] where McBrearty teaches that a typical token "has a limited lifetime, typically 24 hours before the token expires and the user must re-apply for a new token." However, this statement does not teach or suggest determining a default expiration time and if the default expiration time is earlier than the maximum expiration time, setting the expiration time of the access token to be the default expiration time, as recited by Applicants' claim. Instead, McBrearty, whether considered singly or in combination, merely states that typical tokens have a limited lifetime of *typically* 24 hours. Nowhere does McBrearty mention anything about comparing a default expiration time to a maximum expiration time as would be required for McBrearty to teach or suggest setting a token's expiration time to the default expiration time *if the default expiration time is earlier than the maximum expiration time*. Moreover, Schmeidler and Hart fail to overcome this deficiency of McBrearty.

Additionally, the Examiner's combination of Schmeidler, Hart and McBrearty would not result in a method that includes determining a default expiration time and if the default expiration time is earlier than the maximum expiration time, setting the expiration time of the access token to the default expiration time. Instead, the combination would result in a system that sets a token's expiration time as a multiple of the activator's keep-alive time, as taught by Schmeidler, and that also includes time periods during which

individual access functions (e.g., reading, writing or executing) may be disabled for specific users or groups of users, as taught by McBrearty. Thus, the Examiner's combination of cited art would not result in a system or method that includes the limitations of claim 16.

As discussed above, McBrearty does not teach the act of determining of an access token expiration time. McBrearty teaches a token that has a limited lifetime of typically 24 hours, but McBrearty does not describe how this expiration time is determined and McBrearty clearly does not describe the expiration time as a default expiration time. Therefore, McBrearty does not teach the limitations of the Applicants' claims. In addition, the Examiner has failed to address the limitations, **determining a default expiration time; and if the default expiration time is earlier than the maximum expiration time, setting the expiration time of the access token to be the default expiration time** in his remarks. Applicants again assert that these limitations are not taught by the cited references, taken alone or in combination.

Thus, for at least the reasons above, the rejection of claim 16 is not supported by the cited art and removal thereof is respectfully requested. Similar remarks also apply to claims 2, 7 and 12.

Applicants also assert that numerous ones of the dependent claims recite further distinctions over the cited art. However, since the rejections have been shown to be unsupported for the independent claims, a further discussion of the dependent claims is not necessary at this time.

CONCLUSION

Applicants submit the application is in condition for allowance, and notice to that effect is respectfully requested.

If any fees are due, the Commissioner is authorized to charge said fees to Meyertons, Hood, Kivlin, Kowert, & Goetzel, P.C. Deposit Account No. 501505/5760-19800/RCK.

Respectfully submitted,

/Robert C. Kowert/
Robert C. Kowert, Reg. #39,255
Attorney for Applicants

Meyertons, Hood, Kivlin, Kowert, & Goetzel, P.C.
P.O. Box 398
Austin, TX 78767-0398
Phone: (512) 853-8850

Date: December 20, 2007